IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
GALVESTON DIVISION

BEVERLY T. PETERS, individually and on behalf of all others similarly situated, **PLAINTIFF**	
v.	**CASE NO.: 3:14-cv-00114**
ST. JOSEPH SERVICES CORP. d/b/a ST. JOSEPH HEALTH SYSTEM and ST. JOSEPH REGIONAL HEALTH CENTER, **DEFENDANTS**	**JURY TRIAL DEMANDED**

PLAINTIFF'S RESPONSE IN OPPOSITION TO DEFENDANTS' RULE 12(b)(1) MOTION TO DISMISS

TABLE OF CONTENTS

NATURE OF THE CASE.. 1

PETERS' ALLEGATIONS.. 3

STANDARDS OF REVIEW.. 7

A. Rule 12(b)(1) standard.. 7

B. Article III standing.. 8

C. Article III standing in data breach cases.. 11

ARGUMENTS AND AUTHORITIES.. 15

A. Peters' Complaint meets all three prongs of the Article III pleading standard. St. Joseph does not contest the last two prongs of the standard.....15

B. Peters' alleged statutory damages under FCRA confer Article III standing.....17

C. Peters' alleged injury for the lost benefit of the bargain/diminished value of medical services purchased from St. Joseph confer Article III standing 19

D. Peters' alleged injury for deprivation of the value of her PII/PHI confers Article III standing 21

E. Peters' alleged injuries for actual identity theft, identity fraud and/or medical fraud, invasion of privacy, and breach of the confidentiality of her PII/PHI confer Article III standing.....25

F. Peters' alleged injury for emotional distress regarding her compromised PII/PHI and the resulting identity theft, identity fraud and/or medical fraud experienced to date, confers Article III standing.....28

TABLE OF AUTHORITIES

Cases **Page(s)**

Anderson v. Hannaford Bros.,
659 F.3d 151 (1st Cir. 2011).....25

Barnes & Noble Pin Pad Litig.,
No. 12-CV-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013).....11, 12, 24

Blue Water Endeavors, LLC,
Bankr. No. 08–10466, Adv. No. 10–1015, 2011 WL 52525
(E.D. Tex. Jan. 6, 2011).....7

Caudle v. Towers, Perrin, Forster & Crosby, Inc.,
580 F. Supp.2d 273 (S.D.N.Y. 2008) 13

Central Delta Water Agency v. United States,
306 F.3d 938 (9th Cir. 2002) 13

Clapper v. Amnesty Int'l USA,
133 S. Ct. 1138 (2013).....11, 12, 14, 24

Daly v. Metropolitan Life Ins. Co.,
782 N.Y.S.2d 530 (N.Y. Sup. Ct. 2004).....24

Den Norske Stats Oljeselskap As v. HeereMac Vof,
241 F.3d 420 (5th Cir.2001) *cert. denied sub nom*,
Statoil ASA v. HeereMac v.o.f., 534 U.S. 1127 (2002) 7

Denney v. Deutsche Bank AG,
443 F.3d 253 (2d Cir. 2006) 13

Dep't of Veterans Affairs (VA) Data Theft Litig.,
No MISC.A. 06-0506 JR, 2007 WL 7621261.....28, 29

Doe 1 v. AOL,
719 F. Supp.2d 1102 (N.D. Cal. 2010).....13, 24

Facebook Privacy Litig.,
791 F. Supp. 2d 705 (N.D. Cal. 2011).....11, 18

Facebook Privacy Litig.,
No. 12-15619, 2014 WL 1815489 (9th Cir. May 8, 2014) 23

Family Eldercare v. Gilbert,
324 F.3d 383 (5th Cir. 2003) 10

Fed. Election Comm'n v. Akins,
524 U.S. 11 (1998).....10

Graczyk v. West Pub. Co.,
660 F.3d 275 (7th Cir. 2011) 10, 17

Havens Realty Corp. v. Coleman,
455 U.S. 363 (1982).....10

Holmes v. Countrywide Fin. Corp.,
No. 08-CV-00205, 2012 WL 2873892 (W.D. Ky. July 12, 2012).....13, 15, 16

Klimas v. Comcast Cable Comms., Inc.,
465 F.3d 271 (6th Cir. 2006) 10, 18

Krottner v. Starbucks Corp.,
628 F.3d 1139 (9th Cir. 2010) 12

Krottner v. Starbucks Corp.,
No. C09-0216RAJ, 2009 WL 7382290 (W.D. Wash. Aug. 14, 2009)
(*Krottner I*).....13

Lambert v. Hartman,
517 F.3d 433 (6th Cir. 2008) 25

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992).....8, 9, 17, 29

McLoughlin v. People's United Bank, Inc.,
No. 08-CV-00944, 2009 WL 2843269 (D. Conn. Aug. 31, 2009).....13

Moyer v. Michaels Stores,
No. 14-C-561, 2014 WL 3511500 (N.D. Ill. July 14, 2014).....14

Paterson v. Weinberger,
644 F.2d 521 (5th Cir. 1981) 7

People v. Kozlowski,
96 Cal. App. 4th 853 (2002) 24

Pisciotta v. Old Nat. Bancorp,
499 F.3d 629 (7th Cir. 2007) 14

Preminger v. Peake,
552 F.3d 757 (9th Cir. 2008) 9, 17

Ramming v. United States,
281 F.3d 158 (5th Cir. 2001) 7

Resnick v. AvMed, Inc.,
693 F.3d 1317 (11th Cir. 2012) .....*passim*

Richardson v. DSW, Inc.,
Case No. 05 C 4599, 2005 U.S. Dist. LEXIS 26750
(N.D. Ill. Nov. 3, 2005).....23

Ruiz v. Gap, Inc.,
380 Fed. Appx. 689 (9th Cir. 2010).....12

Ruiz v. Gap, Inc.,
622 F.Supp.2d 908 (N.D. Cal. 2009) (*Gap II*).....12

Science Applications International Corp. (SAIC) Backup Tape Data Theft Litig., MDL No. 2360, 2014 WL 1858458
(D.D.C. May 9, 2014) 25, 27, 28, 29

Sierra Club v. E.P.A.,
292 F. 3d 895, 898 (D.C. Cir 2002).....29

Sony Gaming Networks and Customer Data Sec. Breach Litigation,
903 F. Supp.2d 942 (S.D. Cal. Oct. 11, 2012).....21

Sony Gaming Networks & Customer Data Sec. Breach Litigation,
MDL No. 11–2258, 2014 WL 223677 (S.D. Cal. Jan. 21, 2014) 14

Stollenwerk v. Tri-West Health Care Alliance,
254 Fed. Appx. 664 Cir. 2007 16

Susan B. Anthony List v. Driehaus,
No. 13-193, 2014 WL 2675871 (S.Ct. June 16, 2014).....8, 15

U. S. v. Students Challenging Reg. Agency Proc.,
412 U.S. 669 (1973).....9, 10

Warth v. Seldin,
422 U.S. 490 (1975).....*passim*

Williamson v. Tucker,
645 F.2d 404 (5th Cir. 1981) 7

Zappos.com, Inc. Customer Data Security Breach Litigation,
MDL No. 2357, 2013 WL 4830497 (D. Nev. Sept. 9, 2013).....14

Zivotofsky ex rel. Ari Z. v. Sec'y of State,
444 F.3d 614 (D.C. Cir. 2006).....9, 10

Statutes Mentioned

FED. R. CIV. P. 12(b)(1).....*passim*

Cable Act.....11, 18

Driver's Privacy Protection Act 10, 18

Fair Credit Reporting Act 6, 11, 17, 18, 28, 29

Fair Housing Act.....10

Federal Advisory Committee Act 10

Freedom of Information Act 9

Other Authorities

Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013) 23

Charts Sell for $50 Each on Black Market (April 28, 2014),
http://www.medscape.com/viewarticle/824192 (last visited June 26, 2014).....22

John T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*,

15 RICH. J.L. & TECH. 11 (2009) 22

Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) 23

Robert Lowes, "Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market", *http://www.medscape.com* (April 28, 2014) 23

Wolf Richter, "How Much Is My Data Worth? (Google Just offered Me $$)", *http://www.nakedcapitalism.com* 23

TO THE HONORABLE UNITED STATES DISTRICT COURT:

Plaintiff Beverly T. Peters ("Peters"), on behalf of herself and all others similarly situated, files this Response to the FED. R. CIV. P. 12(b)(1) Motion to Dismiss ("MTD") (Doc.# 26) filed by Defendants St. Joseph Services Corporation d/b/a St. Joseph Health System and St. Joseph Regional Health Center (together, "St. Joseph"), and respectfully shows the following:

NATURE OF THE CASE[1]

This is a consumer class action data breach lawsuit seeking redress for St. Joseph's unauthorized disclosure of the highly confidential and personal information of Peters and approximately 405,000 similarly situated persons (*i.e.*, the Class Members). Unlike the typical consumer data breach case only involving personally identifiable information ("PII")—such as, for example, names, addresses, Social Security numbers, and dates of birth—this case, more importantly, also involves protected health information ("PHI")—such as, for example, medical diagnoses, medical treatments, prescribed medications, charts and other medical records. This is a medical data breach case.

Peters and Class Members entrusted their PII/PHI to St. Joseph in connection with purchasing health care services based on St. Joseph's assurances

[1] The "Nature of the Case" section of this Response is taken from Peters' allegations in Paragraphs 1-8 of her First Amended Class Action Complaint (the "Complaint") (Doc. #22).

on its website that the proper data security measures, policies, procedures and protocols were in place and operational to safeguard and protect their PII/PHI. Peters' and Class Members' PII/PHI, however, was improperly handled and stored, inadequately secured, on information and belief, unencrypted, and not kept under applicable, required, and appropriate cyber-security measures, policies, procedures and/or protocols. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, Peters' and Class Members' PII/PHI was stolen and compromised, thereby resulting in economic damages and other injury and harm (the "Data Breach").

Peters is a former St. Joseph patient. The Class Members are current and former St. Joseph patients, employees and some employees' beneficiaries. According to St. Joseph's February 4, 2014 press release revealing the Data Breach, the stolen and compromised PII/PHI include names, Social Security numbers, dates of birth, medical information (*i.e.*, PHI), and possibly addresses.

Rather than stepping up to the plate, taking responsibility for its conduct and the resulting Data Breach, doing the right thing, and addressing the injury and harm inflicted on its current and former patients and employees, St. Joseph asks the Court to summarily dismiss this action. According to St. Joseph, there is no legal claim anywhere under which it is liable to Peters and Class Members for the

economic damages and other injury and harm caused by the Data Breach. For the reasons set forth below, St. Joseph's motion should be denied.

PETERS' ALLEGATIONS[2]

Peters is a former St. Joseph patient who purchased and received health care services from St. Joseph and its affiliated physicians at several of its health care facilities. Peters entrusted her PII/PHI to St. Joseph in connection with purchasing and receiving such health care services based on St. Joseph's assurances on its website that the proper data security measures, policies, procedures and protocols were in place and operational to safeguard and protect her PII/PHI. Peters' PII/PHI, however, was stolen and compromised in the Data Breach—as confirmed by the February 4, 2014 Data Breach notification letter she received from St. Joseph. *See* Exhibit A to the Complaint.

Peters has never been victimized by a data breach other than the St. Joseph Data Breach. She meticulously protects her PII/PHI. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them regularly. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She also maintains her hard copy credit card and financial account statements in a safe for five years, after which she burns them in a trash barrel on her property.

[2] Peters' allegations in this section of the Response are taken from Paragraphs 11-19 of her Complaint.

Peters alleges that as a direct and/or proximate result of the Data Breach, her PII/PHI was accessed and utilized by one or more unauthorized third parties who inflicted identity theft and/or identity fraud by attempting to make unauthorized charges on her Discover card. Peters provided her Discover card account number to St. Joseph on forms she submitted to St. Joseph in connection with purchasing health care services. After the Data Breach, and while she was in Texas, Peters received a text from Discover requesting approval for an unauthorized, out of the ordinary retail purchase in Pennsylvania. When Peters declined to approve the purchase, Discover immediately closed her account, and reissued a new payment card to her. Prior to the Data Breach, Peters never experienced any attempt by fraudsters to access her Discover card account.

Peters further alleges that as a direct and/or proximate result of the Data Breach, she also suffered identity theft and/or identity fraud in the form of the breach of her Yahoo email account which, along with her Social Security number and Texas Driver's License number, was also submitted to St. Joseph in connection with purchasing health care services. All of Peters' online financial, credit card, and retail accounts are linked to her Yahoo email account. After the Data Breach, friends and relatives reported receiving large volumes of spam email from her Yahoo email account. As a result of this fraudulent activity, Peters changed the password on her Yahoo email account. Prior to the Data Breach,

Peters never experienced any attempt by fraudsters to access her Yahoo email account and/or her online financial, credit card, and retail accounts.

Peters further alleges that as a direct and/or proximate result of the Data Breach, she also suffered identity theft and/or identity fraud in the form of the unauthorized access of her Amazon.com account by an unidentified fraudster. Thereafter, another fraudster attempted to access her Amazon.com account using her son's name, which only could have been obtained from her stolen and compromised PHI because St. Joseph required her to provide the names and contact information of her next of kin. Peters' son confirmed he did not attempt to access her Amazon.com account. Prior to the Data Breach, Peters never experienced any attempt by fraudsters to access her Amazon.com account.

Peters further alleges that as a direct and/or proximate result of the Data Breach, she also suffered identity theft, identity fraud and/or medical fraud in the form of multiple telephone solicitations from medical products and services companies asking to speak with specific members of her family. This information only could have been obtained from her stolen and compromised PHI because St. Joseph required her to provide the names and contact information of her next of kin. On the average, Peters receives 2-3 such calls a day at all times of the day and night. Prior to the Data Breach, Peters never received such telephone solicitations.

Peters further alleges that as a direct and/or proximate result of the Data Breach, she also suffered identity theft, identity fraud and/or medical fraud in the form of unsolicited emailed and mailed marketing materials specifically targeting her confidential medical conditions listed in her stolen PII/PHI that the senders only could have learned by obtaining her stolen PII/PHI from the data thieves. Prior to the Data Breach, Peters never received such targeted marketing materials.

Peters further alleges that as a direct and/or proximate result of the Data Breach, she has suffered (and will continue to suffer) economic damages and other actual harm in the form of the deprivation of the value of her PII/PHI, for which there is a well-established national and international market. PII/PHI is a valuable property right. Faced with the choice of having her PII/PHI stolen, compromised, bought, sold and utilized without authorization and receiving compensation versus selling her PII/PHI on the black market and receiving the compensation herself, Peters would choose the latter. Peters asserts that she—not data thieves—should have the exclusive right to monetize her PII/PHI at the highest values possible.

Peters further alleges that as a direct and/or proximate result of the Data Breach, she has suffered (and will continue to suffer) other economic damages and actual harm, including (i) invasion of privacy, (ii) the breach of her confidentiality by the improper disclosure of her PII/PHI without authorization, (iii) statutory damages under FCRA, (iv) lost benefit of her bargain, (v) diminished value of the

medical services she purchased from St. Joseph, and (viii) emotional distress from the compromise of her PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date.

STANDARDS OF REVIEW

A. Rule 12(b)(1) standard.

Rule 12(b)(1) allows a party to move for dismissal of an action for lack of subject matter jurisdiction. As the plaintiff, Peters bears the burden of proof that subject matter jurisdiction exists. *Ramming v. United States*, 281 F.3d 158, 161 (5th Cir. 2001). In reviewing a Rule 12(b)(1) motion, the Court may consider (i) the complaint alone, (ii) the complaint supplemented by undisputed facts evidenced in the record, or (iii) the complaint supplemented by undisputed facts plus the court's resolution of disputed facts. *Williamson v. Tucker*, 645 F.2d 404, 413 (5th Cir. 1981).

A Rule 12(b)(1) motion to dismiss is either a "facial" attack (*i.e.*, the allegations are insufficient to invoke federal jurisdiction), or a "factual" attack (*i.e.*, the facts supporting subject matter jurisdiction are questioned). *In re Blue Water Endeavors, LLC*, Bankr. No. 08–10466, Adv. No. 10–1015, 2011 WL 52525, *3 (E.D. Tex. Jan. 6, 2011) (citation omitted). A facial attack happens when a defendant files a Rule 12(b)(1) motion without accompanying evidence. *Paterson v. Weinberger*, 644 F.2d 521, 523 (5th Cir. 1981). In a facial attack, the Court

must assume all allegations are true. *Den Norske Stats Oljeselskap As v. HeereMac Vof*, 241 F.3d 420, 424 (5th Cir.2001) *cert. denied sub nom, Statoil ASA v. HeereMac v.o.f.*, 534 U.S. 1127 (2002).

Here St. Joseph mounts a Rule 12(b)(1) facial attack on Peters' Complaint, arguing Peters asserts no cognizable injury supporting Article III standing. MTD at 3. St. Joseph is wrong.

B. Article III standing.

Article III standing "in no way depends on the merits of the plaintiff's contention that particular conduct is illegal." *Warth v. Seldin*, 422 U.S. 490, 500 (1975); *In re Deepwater Horizon-Appeals of the Economic and property Damage Class Action Settlement*, No. 13-30095, 2014 WL 2118614, at *1 (5th Cir. May 19, 2014) ("[F]ederal courts are not limited by the parties' contentions when acting on Article III jurisdiction.") (citation omitted). Indeed, regarding motions to dismiss, courts "presume that general allegations embrace those specific facts that are necessary to support the claim." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) (quotations omitted).

"To establish Article III standing, a plaintiff must show (1) an injury in fact (2) a sufficient causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision." *Susan B. Anthony List v. Driehaus*, No. 13-193, 2014 WL 2675871, at *5 (S.Ct.

June 16, 2014) (internal quotations omitted). "An injury sufficient to satisfy Article III must be concrete and particularized and actual or imminent, not conjectural or hypothetical." *Susan B. Anthony List,* 2014 WL 2675871, at *5.

"Injury in fact" reflects the requirement that a person be "adversely affected" or "aggrieved," and distinguishes a person with a direct stake in the outcome of a litigation—even though small—from a person with a mere interest in the problem. *U. S. v. Students Challenging Reg. Agency Proc.*, 412 U.S. 669, 690 n. 14 (1973).

"The injury may be minimal." *Preminger v. Peake*, 552 F.3d 757, 763 (9th Cir. 2008). Indeed, the injury-in-fact requirement can be satisfied "solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'" *Lujan*, 504 U.S. 555, 578 (1992). Stated alternatively, the legislature "may create a statutory right or entitlement the alleged deprivation of which can confer standing to sue even where the plaintiff would have suffered no judicially cognizable injury in the absence of statute." *Warth,* 422 U.S. at 514; *Lujan*, 504 U.S. at 578.

For example, in *Zivotofsky ex rel. Ari Z. v. Sec'y of State*, 444 F.3d 614 (D.C. Cir. 2006), the court used a Freedom of Information Act violation to demonstrate how the mere violation of a statute can confer standing, holding that "[a]nyone whose request for specific information has been denied has standing to bring an action; the requester's circumstances—why he wants the information, what he

plans to do with it, what harm he suffered from the failure to disclose—are irrelevant to his standing." *Id.*, 444 F.3d at 617-18. As the *Zivotofsky* further held:

> Although it is natural to think of an injury in terms of some economic, physical, or psychological damage, a concrete and particular injury for standing purposes can also consist of the violation of an individual right conferred on a person by statute. Such an injury is concrete because it is of "a form traditionally capable of judicial resolution," [citation omitted] and it is particular because, as the violation of an *individual* right, it "affect[s] the plaintiff in a personal and individual way."

Id., 444 F.3d at 618-19; *see also Students Challenging Reg. Agency Proc.*, 412 U.S. at 686 (standing is not confined to only those who can show economic harm).

The Supreme Court has held that "a plaintiff suffers an 'injury in fact' when the plaintiff fails to obtain information which must be publicly disclosed pursuant to a statute." *Fed. Election Comm'n v. Akins*, 524 U.S. 11, 21 (1998) (failure to disclose information under Federal Advisory Committee Act "constitutes sufficient distinct injury to provide standing to sue"); *see also Havens Realty Corp. v. Coleman*, 455 U.S. 363, 374 (1982) (injury in fact existed when information required under the Fair Housing Act was withheld); *Grant ex rel. Family Eldercare v. Gilbert*, 324 F.3d 383, 387 (5th Cir. 2003) (citing *Akins*).

Courts have also routinely found injury-in-fact where a plaintiff alleges the violation of a consumer privacy statute with a private right of action. *See e.g.*, *Graczyk v. West Pub. Co.*, 660 F.3d 275, 278 (7th Cir. 2011) (finding monetary harm not necessary to state a claim under the Driver's Privacy Protection Act, as

"Congress has defined the relevant injury under the DPPA as the 'obtain[ment], disclos[ure], or [use]'") (citation omitted); *Klimas v. Comcast Cable Comms., Inc.*, 465 F.3d 271, 275-76 (6th Cir. 2006) (standing exists where a plaintiff alleges violations of the Cable Act's privacy provisions, even absent economic harm); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011).

C. Article III standing in data breach cases.

St. Joseph cites *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) (applying *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013)) as the overarching Article III standard in data breach cases. MTD at 4-7. This is a much too simplistic approach.

A careful reading of St. Joseph's briefing of *Barnes & Noble* and *Clapper* in this section will confirm it is limited to data breach injury in the form of an "increased risk of additional real and impending future economic damages and other actual harm." While this is type of data breach injury is serious, it is not by any means the only type of data breach injury—and it certainly is not the only injury Peters alleges. *See, e.g.*, Complaint, ¶¶ 13-19, 54, 77, 81, 85, 90, 100, 105, 120, 126, 137, 141, and 148 (alleging economic damages and other actual harm in the form of, *inter alia*, (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under FCRA, (v) lost benefit of their bargains, (vi) deprivation

of the value of their PII/PHI, for which there is a well-established national and international market, (vii) diminished value of the medical services they purchased from St. Joseph, and (viii) emotional distress from the compromise of their PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date).

A proper analysis of standing in a consumer data breach case is much more nuanced than St. Joseph's approach. It is not enough to shout *Barnes & Noble* and *Clapper* from the rooftops, and call it a day. Each case turns on its own unique facts and allegations. Each pleaded injury must be analyzed within its context and the law. An overarching Article III standing standard that applies across the board in all data breach cases does not exist.

That said, regarding Peters alleged injury in the form of "the increased risk of additional real and impending future economic damages and other actual harm" (Complaint, ¶44) supports Article III standing. Indeed, since *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 633–34 (7th Cir. 2007), with limited exceptions due to pleading deficiencies not existing here, courts have routinely recognized that a plausibly pled increased risk of identity theft supports an injury-in-fact finding supporting Article III standing in data breach cases. *See, e.g.*, *Ruiz v. Gap, Inc.*,

380 Fed. Appx. 689, 690-91 (9th Cir. 2010); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142–43 (9th Cir. 2010).[3] This trend continues post-*Clapper*.

For example, in *Moyer v. Michaels Stores*, No. 14-C-561, 2014 WL 3511500 (N.D. Ill. July 14, 2014), plaintiffs asserted they suffered the following injuries in support of Article III standing: (i) an elevated risk of identity theft and costs associated with protecting themselves against this risk, (ii) overpayment for goods that Michaels allegedly priced to reflect the added cost of securing credit and debit card information, (iii) a lost property interest in their personal identifying information and its alleged commercial value, and (iv) "additional ... monetary losses arising from unauthorized bank account withdrawals, fraudulent card payments, and/or related bank fees charged to their accounts." *Id*. at *4. Like St. Joseph, Michaels Stores argued for dismissal for lack of standing, asserting *Clapper*. The court, in *Moyer*, found otherwise:

> [T]he elevated risk of identity theft stemming from the data breach at Michaels is sufficiently imminent to give Plaintiffs standing. This

[3] *See also Holmes v. Countrywide Fin. Corp.*, No. 08-CV-00205, 2012 WL 2873892, at *5-*11(W.D. Ky. July 12, 2012); *McLoughlin v. People's United Bank, Inc.*, No. 08-CV-00944, 2009 WL 2843269, at *3-*4 (D. Conn. Aug. 31, 2009); *Doe 1 v. AOL*, 719 F. Supp.2d 1102, 1109–11 (N.D. Cal. 2010); *Ruiz v. Gap, Inc*., 622 F.Supp.2d 908, 912 (N.D. Cal. 2009) (*Gap II*); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp.2d 273, 280 (S.D.N.Y. 2008); *Krottner v. Starbucks Corp*., No. C09-0216RAJ, 2009 WL 7382290, at *4 (W.D. Wash. Aug. 14, 2009) (*Krottner I*); *accord Denney v. Deutsche Bank AG*, 443 F.3d 253, 264 (2d Cir. 2006); *Central Delta Water Agency v. United States*, 306 F.3d 938, 947 (9th Cir. 2002).

> conclusion follows from *Pisciotta* and is consistent with a host of Supreme Court decisions finding standing based on an imminent risk of future injury. *Clapper* is distinguishable based on its admittedly rigorous application of the "certainly impending" standard in a case that involved (1) national security and constitutional issues and (2) no evidence that the relevant risk of harm had ever materialized in similar circumstances.

Id. at *6. Peters' allegations are much more detailed than those alleged in *Moyer*.

Likewise, *In re Sony Gaming Networks & Customer Data Sec. Breach Litigation,* MDL No. 11–2258, 2014 WL 223677, at *9 (S.D. Cal. Jan. 21, 2014), another post-*Clapper* data breach case ruling, the court found Article III standing based on a "plausibly alleged ... 'credible threat' of impending harm."

In *In re Zappos.com, Inc. Customer Data Security Breach Litigation*, MDL No. 2357, 2013 WL 4830497 (D. Nev. Sept. 9, 2013),[4] thieves hacked into Zappos.com's computer system and stole customer names, account numbers, account passwords, email addresses, billing and shipping addresses, telephone numbers and the last four digits of customer credit cards. The court found plaintiffs had standing because they "sufficiently alleged that they have had to pay money to monitor their credit scores and secure their financial information due to the increased risk of criminal fraud against them occasioned by Defendant's negligent loss of their personal information." *Id*. at *2.

[4] Richard L. Coffman, one of Peters' counsel, is Co-lead Class Counsel in the *Zappos.com* data breach litigation.

Here, and besides the increased risk of criminal fraud due to St. Joseph's wrongful disclosure of her PII/PHI, Peters alleges several other injuries directly and/or proximately caused by the Data Breach. As discussed in greater detail below, any one of these injuries confers Article III standing on Peters.

ARGUMENTS AND AUTHORITIES

A. Peters' Complaint meets all three prongs of the Article III pleading standard. St. Joseph does not contest the last two prongs of the standard.

In order to establish Article III standing, Peters must demonstrate that (i) she has suffered a concrete and particularized injury that is either actual or imminent, (ii) the injury is fairly traceable to St. Joseph, and (iii) it is likely a favorable decision will redress the injury. *Susan B. Anthony List*, 2014 WL 2675871, at *5.

St. Joseph's analysis of Peters' alleged injuries focuses only on the first prong of the standard—concrete and particularized injury. St. Joseph concedes the second prong (other than invasion of privacy) and third prong of the standard.

As discussed below, Peters' alleged injuries are concrete and particularized.

Peters' injuries also are fairly traceable to St. Joseph's wrongful conduct. She meticulously protects her PII/PHI. Complaint, ¶12. She has never been victimized by a data breach other than the St. Joseph Data Breach. *Id.* An injury even *indirectly* caused by a defendant's actions satisfies the fairly traceable

requirement. *See, e.g.*, *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1324 (11th Cir. 2012); *Holmes*, 2012 WL 2873892, at *5.

Incredibly, of all her alleged injuries, St. Joseph argues—via conclusory statements—that Peters' invasion of privacy injury is not traceable to the Data Breach. MTD at 11-12. St. Joseph offers no explanation why—just that it isn't. *Id*. St. Joseph is wrong. Even the court, in *Stollenwerk*, recognized:

> [P]roximate cause is supported not only by the temporal, but also by the *logical*, relationship between the two events… . As a matter of twenty-first century common knowledge, just as certain exposures can lead to certain diseases, the theft of a computer hard drive certainly can result in an attempt by a thief to access the contents for purposes of identity fraud, and such an attempt *can* succeed… . Given all these circumstances, a reasonable jury could, on the present record, find it more likely than not that a causal relationship existed between the burglary and the incidents of identity theft.

Stollenwerk v. Tri-West Health Care Alliance, 254 Fed. Appx. 664, 668 9th Cir. 2007) (a data breach case). *See also Resnick*, 693 F.3d at 1324 (a "showing that an injury is 'fairly traceable' requires less than a showing of '"proximate cause"').

Here, the alleged misuse of Peters' stolen and compromised PII/PHI began *after* "St. Joseph *intentionally invaded Plaintiff's and Class Members' privacy* by disseminating their PII/PHI to the world by repeatedly failing and refusing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, protocols, and software and hardware systems to ensure the

security and confidentiality of their PII/PHI." Complaint, ¶125. Peters' invasion of privacy injury is fairly traceable to the Data Breach.

Finally, a favorable court decision will redress Peter's injury. *Resnick*, 693 F.3d at 1324 ("Plaintiffs allege a monetary injury and an award of compensatory damages would redress that injury. Plaintiffs have alleged sufficient facts to confer standing…."). St. Joseph does not challenge this prong of the Article III inquiry. It is, therefore, undisputed that Peters seeks damages and injunctive relief that, if she is successful, will redress her claims and achieve the desired results. See Complaint, ¶¶ 148-51.

B. Peters' alleged statutory damages under FCRA confer Article III standing.

For Article III standing, "[t]he injury may be minimal." *Preminger*, 552 F.3d at 763. Indeed, the injury-in-fact requirement can be satisfied "solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'" *Lujan*, 504 U.S. at 578. Thus, the legislature "may create a statutory right or entitlement the alleged deprivation of which can confer standing to sue even where the plaintiff would have suffered no judicially cognizable injury in the absence of statute." *Id*.; *Warth*, 422 U.S. at 514.

Peters alleges violations of FCRA (Complaint, ¶¶66-81), a federal statute with a private right of action. Her alleged FCRA statutory damages vest her with Article III standing. Courts throughout the country routinely find injury-in-fact

where a plaintiff alleges a violation of a consumer privacy statute with a private right of action. *See e.g.*, *Graczyk v. West Pub. Co.*, 660 F.3d 275, 278 (7th Cir. 2011) (finding monetary harm not necessary to state a claim under the Driver's Privacy Protection Act, as "Congress has defined the relevant injury under the DPPA as the 'obtain[ment], disclos[ure], or [use]'of an individual's personal information") (citations omitted); *Klimas v. Comcast Cable Comm'ns., Inc.,* 465 F.3d 271, 275–76 (6th Cir. 2006) (standing existed where plaintiff alleged violations of the Cable Act privacy provisions, even absent economic harm); *In re Facebook Privacy Litig.*, 791 F. Supp.2d 705, 712 (N.D. Cal. 2011).

St. Joseph, however, does not address this longstanding legal principle or these cases. Rather, St. Joseph argues that Peters' alleged statutory damages under FCRA do not confer Article III standing because she fails to state a valid FCRA claim. MTD at 15-16. But this argument is circular. It is addressed in Peters' response to St. Joseph's Rule 12(b)(6) motion to dismiss (which Peters incorporates by reference). Article III standing "in no way depends on the merits of the plaintiff's contention that particular conduct is illegal." *Warth*, 422 U.S. at 500. Nowhere in its MTD does St. Joseph address the fundamental truth that courts throughout the country routinely find injury-in-fact where a plaintiff alleges the violation of a statute with a private right of action.

C. Peters' alleged injury for lost benefit of the bargain/diminished value of medical services purchased from St. Joseph confer Article III standing.

Peters asserts St. Joseph "breached its implied contracts with Plaintiff and Class Members and directly and/or proximately caused them to suffer economic damages and other actual harm in the form of, *inter alia*, the lost benefit of their bargains; to wit, they understood, agreed and expected that a portion of the price they paid to St. Joseph for health care services would be spent by St. Joseph to safeguard and protect their PII/PHI—especially in light of St. Joseph's representations in its Privacy Notice [on the website]." Complaint, ¶115. "Although Plaintiff and Class Members paid for protection of their PII/PHI, St. Joseph failed to do so, thereby resulting in its theft and dissemination to the world and Plaintiff's and Class Members' lost benefit of their bargains." *Id*.

Peters also asserts "St. Joseph holds money conferred on it by Plaintiff and Class Members—*i.e*., that portion of the health services purchase prices Plaintiff and Class Members paid St. Joseph for protecting their PII/PHI, which St. Joseph admittedly failed to do." Complaint, ¶144. "St. Joseph has been unjustly enriched by the funds it should have spent to safeguard and protect their PII/PHI which, in equity and good conscience, belongs to Plaintiff and Class Members, and should be refunded, because St. Joseph failed to do so." *Id*.

Peters' alleged injury for lost benefit of the bargain/diminished value of medical services purchased is precisely the type of economic damage recognized

by the Eleventh Circuit Court of Appeals as an injury-in-fact conferring Article III standing in a data breach case. *See Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012), a case St. Joseph conveniently omits from its motion. In fact, the Eleventh Circuit's ruling ultimately drove a $3 million settlement. *See* http://www.databreachsettlement.com/faq (last visited August 14, 2014).

In *Resnick*, current and former members of health care plans sued the operator of the plans pertaining to a data breach in which unencrypted laptops containing their sensitive information were stolen from the plan operator's corporate office. Plaintiffs asserted, among other claims, a claim for restitution/unjust enrichment.

Plaintiffs alleged AvMed could not equitably retain their monthly health insurance premiums—part of which was intended to pay for the administrative costs of data security—because AvMed did not properly secure their data—as demonstrated by the fact that the stolen laptops were unencrypted. *Id*., 693 F.3d at 1328. Similar to Peters, plaintiffs, in Av Med, alleged (i) they conferred a monetary benefit on AvMed in the form of monthly premiums, (ii) AvMed "appreciates or has knowledge of such benefit," (iii) AvMed uses the premiums to "pay for the administrative costs of data management and security," and (iv) AvMed "should not be permitted to retain the money belonging to Plaintiffs ... because [AvMed] failed to implement the data management and security measures

that are mandated by industry standards." *Id.* Plaintiffs also alleged AvMed either failed to implement or inadequately implemented policies to secure sensitive information, as can be seen from the data breach. *Id.*

AvMed argued the district court correctly dismissed the complaint because plaintiffs' alleged injuries were not cognizable under the law, and because plaintiffs paid AvMed for health insurance, not data security. *Id.*

The Eleventh Circuit agreed with plaintiffs and reversed, in part, the district court's ruling, stating that "[a]ccepting these allegations as true, we find that Plaintiffs alleged sufficient facts to allow this [restitution/unjust enrichment] claim to survive a motion to dismiss." *Id.*

Peters has standing here for the same reasons plaintiffs had standing in *Resnick. See also In re: Sony Gaming Networks and Customer Data Sec. Breach Litigation*, 903 F. Supp.2d 942, 966 (S.D. Cal. Oct. 11, 2012) (economic injury occurs when a plaintiff gives more, or acquires less, in a transaction than he or she otherwise would have).

D. Peters' alleged injury for deprivation of the value of her PII/PHI confers Article III standing.

Peters alleges she "has suffered (and will continue to suffer) economic damages and other actual harm in the form of the deprivation of the value of her PII/PHI, for which there is a well-established national and international market." *See, e.g.*, Complaint, ¶18.

PII/PHI is a valuable property right. *See* Complaint, ¶18 (citing, at note 1, John T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-*4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted)). It is so valuable to identity thieves that once PII has been compromised, criminals often trade it on the "cyber black-market" for several years. Complaint, note 1.

Theft of PHI is also gravely serious; to wit, "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. *Id*. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected." *Id*. (citing Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 27, 2014)). Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market to target market their products and services to the physical maladies of the data breach victims themselves—which Peters also alleges here. Complaint, ¶¶16-17; note 1. Insurance companies purchase and use stolen PHI to adjust their insureds' medical insurance premiums. *Id* at note 1.

The value of PHI as a commodity also is measurable. *See, e.g.*, Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market* (April 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited June 26, 2014); Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013) (all-inclusive health insurance dossiers containing sensitive PII/PHI are fetching $1,200 to $1,300 each), http://www.scmagazine.com/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/article/303302/ (last visited June 26, 2014).[5]

Courts have recognized property rights in the private information of consumers, thereby giving rise to compensable interests. Here, Peters lost her PII/PHI, and thus, her property interest, when St. Joseph failed to adequately secure it. *See In re Facebook Privacy Litig.*, No. 12-15619, 2014 WL 1815489, at *1 (9th Cir. May 8, 2014) (overturning the district court's dismissal of plaintiffs' breach of contract and fraud claims, finding plaintiffs' allegations that they lost the

[5] *See also* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/news/articles/SB10001424052748703529004576160764037920274?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748703529004576160764037920274.html&fpid=2,7,121,122,201,401,641,1009 ("Allow Ltd. . . . offers to sell people's personal information on their behalf, and give them 70% of the sale"). Additionally, consumers can exchange their data for free services, such as Facebook, or sell their data for cash. *See* Wolf Richter, *How Much Is My Private Data Worth? (Google Just Offered Me $$)* (http://www.nakedcapitalism.com/2013/11/wolf-richter-how-much-is-my-private-data-worth-google-just-offered-me.html) (last visited on June 18, 2014).

value of their PII when Facebook wrongly disseminated it was wholly sufficient to confer standing). *See also Richardson v. DSW, Inc.*, Case No. 05 C 4599, 2005 U.S. Dist. LEXIS 26750, at *10 (N.D. Ill. Nov. 3, 2005) (in a data breach case involving stolen credit and debit cards, the court found plaintiff pled a valid breach of implied contract claim where defendant "not only offered to accept certain forms of non-cash payment in exchange for shoes but also offered to take reasonable measures to keep this information secure."); *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1111-12 (N.D. Cal. 2010) (denying motion for judgment on the pleadings based on finding that plaintiffs were injured by public disclosure of their confidential information in violation of defendant's obligation to safeguard same); *Daly v. Metropolitan Life Ins. Co.*, 782 N.Y.S.2d 530, 532, 535 (N.Y. Sup. Ct. 2004) ("[T]his court is convinced that Met Life had a duty to protect the confidential personal information provided by plaintiffs."); *People v. Kozlowski*, 96 Cal. App. 4th 853, 866-67 (2002) (finding that a person's ATM PIN code constitutes valuable intangible property in the context of extortion).

St. Joseph's argument to the contrary (MTD at 8-9) ignores 21st Century reality that markets for PII/PHI exist and are thriving on the black market, ignores the above legal precedent, simplistically leans on *Barnes & Noble* and *Clapper* yet again. As demonstrated by her allegations, and the above-cited articles and case law, there is a well-established robust national and international market for her PII/PHI, she can tap into the market, and "[f]aced with the choice of having her

PII/PHI stolen, compromised, bought, sold and utilized without authorization and receiving compensation versus selling her PII/PHI on the black market and receiving the compensation herself, Peters would choose the latter."[6] Complaint, ¶18. Peters' alleged injury for deprivation of the value of her PII/PHI confers Article III standing.

E. Peters' alleged injuries for actual identity theft, identity fraud and/or medical fraud, invasion of privacy, and breach of the confidentiality of her PII/PHI confer Article III standing.

Actual identity theft, fraud and misuse—such as the identity theft, fraud and misuse Peters pleads here—support a finding of Article III standing. *See Resnick*, 693 F.3d at 1323; *Anderson v. Hannaford Bros.*, 659 F.3d 151, 162-67 (1st Cir. 2011); *Lambert v. Hartman*, 517 F.3d 433, 438 (6th Cir. 2008); *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litig.*, MDL No. 2360, 2014 WL 1858458, at *13 (D.D.C. May 9, 2014).

Here, it is indisputable the Data Breach occurred. Peters describes how she meticulously protects her PII/PHI. Complaint, ¶12. Peters asserts she "has never been victimized by a data breach other than the St. Joseph Data Breach." *Id*.

[6] St. Joseph argues Peters "does not allege [her] personal PII/PHI was actually sold by anyone." MTD at 9. This is false. *See, e.g.*, Complaint, ¶45 ("During the intervening period between the Data Breach and the date the Data Breach notification letters were sent to Plaintiff and Class Members, *their unencrypted PII/PHI, on information and belief, was bought and sold several times on the robust international cyber black market*—as evidenced by the identity theft, identity fraud and/or medical fraud Plaintiff has already suffered … .")(emphasis added).

Peters also asserts she has suffered actual identity theft, identity fraud and/or medical fraud. Complaint, ¶¶ 13-19, 54, 77, 81, 85, 90, 100, 105, 120, and 148.

While St. Joseph argues to the contrary (MTD at 14-15), it conflates the terms identity theft, identity fraud and/or medical fraud. Identity theft occurs when a person's PII/PHI is used without authorization to commit fraud or other crimes—*i.e.*, identity fraud. Complaint, ¶24. On the other hand, medical fraud occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. *Id.*, ¶27.

Here, Peters alleges identity fraud in the form of unauthorized Discover card charges (*id.*, ¶13), the actual breach of her Yahoo email account (which is linked to her online financial, credit card, and retail accounts) (*id.*, ¶14), and the unauthorized access of her Amazon.com account (*id.*, ¶15). St. Joseph glosses over Peters' alleged identity fraud, labeling it "attempted." In doing so, St. Joseph loses sight of the fact that even if identity fraud is *attempted*, logic dictates that identity theft must have occurred in order for the fraudster to obtain the victim's PII/PHI—which, at the very least, happened here. Without the theft of Peters' identity, the alleged identity fraud could not have occurred.

The same is true with Peters' alleged medical fraud in the form of multiple telephone solicitations (2-3 calls per day) from medical products and services companies asking to speak with specific members of her family (*id.*, ¶16), and

unsolicited emailed and mailed marketing materials specifically targeting the medical conditions in her stolen PII/PHI that the senders only could have learned by obtaining her stolen PII/PHI, which she never received prior to the Data Breach (*id*., ¶17). Moreover, this is precisely the type of medical fraud supporting Article III standing for plaintiff Yarde *In re Science Applications Intern'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 2014 WL 1858458, at *13.[7]

An invasion of privacy[8] is much like a breach of confidentiality—they are both legal claims, as well as injuries resulting from the wrongful activity giving rise to the legal claims. Once one's privacy is invaded or confidentiality is breached, they cannot be regained; the victim is *per se* injured. This is especially true in the case of a medical data breach because there is no opportunity for a clean start. Complaint, note 2. Once a victim's PHI is out—such as Peters' and Class

[7] Mr. Coffman also was Co-Lead Class Counsel on behalf of plaintiffs in *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, which was recently settled. Plaintiff Dorothy Yarde was his client.

[8] Regarding Peters' invasion of privacy injury, St. Joseph claims Peters "does not contend that St. Joseph willfully and intentionally disclosed" her PII/PHI. MTD at 12. This statement is false. *See, e.g*., Complaint, ¶125 ("*St. Joseph intentionally invaded Plaintiff's and Class Members' privacy by disseminating their PII/PHI to the world* by repeatedly failing and refusing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, protocols, and software and hardware systems to ensure the security and confidentiality of their PII/PHI.") (emphasis added). *See also id*., ¶4 ("St. Joseph flagrantly disregarded Plaintiff's and Class Members' privacy rights by intentionally, willfully, … failing to take the necessary precautions required to safeguard and protect their PII/PHI from unauthorized disclosure.").

Members' PHI—it is out forever. *Id*. If there is a negative stigma associated with a victim's PHI—such as a sexually-transmitted disease, an abortion, a sex change operation or a slow-growing cancer—it cannot be undone. *Id*.

Even worse, the consequences of having one's PHI fall into the hands of unscrupulous individuals can literally be life threatening. *Id*. When a thief uses a victim's PHI to obtain medical care, the imposter's information could end up on the victim's medical record. *Id*. If the PHI theft victim subsequently was involved in an accident and rushed to the emergency room, doctors utilizing his or her PHI could see the wrong blood type, not know the victim is allergic to certain medications, and/or has a pre-existing condition—which, in turn, could lead to misdiagnosis or mistreatment with potentially deadly consequences. *Id*.

St. Joseph's superficial briefing (MTD at 11-15) simply regurgitates the standard; it provides no insight or thought provoking analysis.

F. Peters' alleged injury for emotional distress regarding her compromised PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date, confers Article III standing.

Adverse effects of a data breach, such as inconvenience, unfairness, and mental distress, also support Article III standing. *See, e.g., In re Dep't of Veterans Affairs (VA) Data Theft Litig*., No. MISC.A. 06-0506 JR, 2007 WL 7621261, at *3 (D.D.C. Nov. 16, 2007).

Similar to its argument regarding her alleged FCRA statutory damages, St. Joseph argues that Peters' alleged emotional distress does not support Article III standing because her claims are conclusory and she fails to allege facts supporting an emotional distress claim. MTD at 10. St. Joseph makes this argument focusing on possible future emotional distress (*id*.) while, at the same time, conveniently sidestepping the emotional distress Peters has already suffered in conjunction with the injuries and harm she has already suffered. Again, St. Joseph's argument is bad form because Article III standing "in no way depends on the merits of the plaintiff's contention that particular conduct is illegal." *Warth*, 422 U.S. at 500.

The government also employed this tactic in *In re Dep't of Veterans Affairs (VA) Data Theft Litig*., denouncing plaintiffs' allegations for failing "to specify the particular individuals who have suffered injuries or to provide any further detail about the injuries alleged." *Id.*, 2007 WL 7621261, at *3. The court rejected the government's argument, found Article III standing, and held that at the pleading stage, "general factual allegations of injury resulting from the defendant's conduct may suffice." *Id*. (citing *Sierra Club v. E.P.A.*, 292 F.3d 895, 898 (D.C. Cir. 2002) (quoting *Lujan*, 504 U.S. at 561)). St. Joseph's arguments against Peters' alleged emotional distress injury should be rejected for the same reason.

WHEREFORE, Plaintiff Beverly T. Peters, on behalf of herself and Class Members, respectfully requests this Court to (i) find she has Article III standing to

assert her claims and causes of action against St. Joseph, (ii) deny St. Joseph's Rule 12(b)(1) motion to dismiss, and (iii) grant her such other and further relief to which she is justly entitled.

Date: August 29, 2014

Respectfully submitted,

/s/ Richard L. Coffman
Richard L. Coffman
THE COFFMAN LAW FIRM
Texas Bar No. 04497460
Federal Bar No. 12055
505 Orleans St., Ste. 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

Mitchell A. Toups
WELLER, GREEN, TOUPS & TERRELL, LLP
Texas Bar No. 20151600
Federal Bar No. 2457
2615 Calder Ave., Suite 400
Beaumont, TX 77702
Telephone: (409) 838-0101
Facsimile: (409) 838-6780
Email: matoups@wgttlaw.com

Jason Webster
THE WEBSTER LAW FIRM
Texas Bar No. 24033318
Federal Bar No. 568715
6200 Savoy, Suite 515
Houston, TX 77036
Telephone: (713) 581-3900
Facsimile: (713) 409-6464
Email: jwebster@thewebsterlawfirm.com

CERTIFICATE OF SERVICE

I certify that a true and correct copy of Plaintiff's response to Defendants' Rule 12(b)(1) Motion to Dismiss was served on the following counsel of record, via the Court's ECF System, on August 29, 2014.

/s/ *Richard L. Coffman*
Richard L. Coffman

Kent Adams
Kristie Johnson
LEWIS BRISBOIS BISGAARD & SMITH, LLP
Weslayan Tower, Suite 1400
24 East Greenway Plaza
Houston, Texas 77046
Telephone: (713) 659-6767
Facsimile: (713) 759-6830
Email: Kent.adams@lewisbrisbois.com
Email: Kristie.johnson@lewisbrisbois.com

ATTORNEYS FOR DEFENDANTS